Dialogic® BorderNet™ 4000 Session Border Controller

3.1.0 Release Notes

July 2013

Copyright and Legal Notice

Copyright © 2011-2013 Dialogic Inc. All Rights Reserved. You may not reproduce this document in whole or in part without permission in writing from Dialogic Inc. at the address provided below.

All contents of this document are furnished for informational use only and are subject to change without notice and do not represent a commitment on the part of Dialogic Inc. and its affiliates or subsidiaries ("Dialogic"). Reasonable effort is made to ensure the accuracy of the information contained in the document. However, Dialogic does not warrant the accuracy of this information and cannot accept responsibility for errors, inaccuracies or omissions that may be contained in this document.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH DIALOGIC® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN A SIGNED AGREEMENT BETWEEN YOU AND DIALOGIC, DIALOGIC ASSUMES NO LIABILITY WHATSOEVER, AND DIALOGIC DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF DIALOGIC PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY INTELLECTUAL PROPERTY RIGHT OF A THIRD PARTY.

Dialogic products are not intended for use in certain safety-affecting situations. Please see http://www.dialogic.com/company/terms-of-use.aspx for more details.

Due to differing national regulations and approval requirements, certain Dialogic products may be suitable for use only in specific countries, and thus may not function properly in other countries. You are responsible for ensuring that your use of such products occurs only in the countries where such use is suitable. For information on specific products, contact Dialogic Inc. at the address indicated below or on the web at *www.dialogic.com*.

It is possible that the use or implementation of any one of the concepts, applications, or ideas described in this document, in marketing collateral produced by or on web pages maintained by Dialogic may infringe one or more patents or other intellectual property rights owned by third parties. Dialogic does not provide any intellectual property licenses with the sale of Dialogic products other than a license to use such product in accordance with intellectual property owned or validly licensed by Dialogic and no such licenses are provided except pursuant to a signed agreement with Dialogic. More detailed information about such intellectual property is available from Dialogic's legal department at 6700 de la Cote-de-Liesse Road, Suite 100, Borough of Saint-Laurent, Montreal, Quebec, Canada H4T 2B5. **Dialogic encourages all users of its products to procure all necessary intellectual property licenses required to implement any concepts or applications and does not condone or encourage any intellectual property infringement and disclaims any responsibility related thereto. These intellectual property licenses may differ from country to country and it is the responsibility of those who develop the concepts or applications to be aware of and comply with different national license requirements.**

Dialogic, Dialogic Pro, Dialogic Blue, Veraz, Brooktrout, Diva, BorderNet, PowerMedia, ControlSwitch, I-Gate, Mobile Experience Matters, Network Fuel, Video is the New Voice, Making Innovation Thrive, Diastar, Cantata, TruFax, SwitchKit, Eiconcard, NMS Communications, SIPcontrol, Exnet, EXS, Vision, inCloud9, NaturalAccess and Shiva, among others as well as related logos, are either registered trademarks or trademarks of Dialogic Inc. and its affiliates or subsidiaries. Dialogic's trademarks may be used publicly only with permission from Dialogic. Such permission may only be granted by Dialogic's legal department at 6700 de la Cote-de-Liesse Road, Suite 100, Borough of Saint-Laurent, Montreal, Quebec, Canada H4T 2B5. Any authorized use of Dialogic's trademarks will be subject to full respect of the trademark guidelines published by Dialogic from time to time and any use of Dialogic's trademarks requires proper acknowledgement.

The names of actual companies and products mentioned herein are the trademarks of their respective owners.

This document discusses one or more open source products, systems and/or releases. Dialogic is not responsible for your decision to use open source in connection with Dialogic products (including without limitation those referred to herein), nor is Dialogic responsible for any present or future effects such usage might have, including without limitation effects on your products, your business, or your intellectual property rights.

Table of Contents

Release 3.1.0 5

Release Version Compatibility Table 5

Maintenance Window Requirements 5

New Functionality 6

Overlapped IP Address 6

IPPBX Registration Support 6

IPsec Support 6

External DNS Support 6

Emergency Services 7

Flexible Media Routing 7

Enterprise Routing 7

Filter Option for Reports 7

User Security Enhancement 7

List Users Currently Logged In With Ability to Close Sessions 7

Resolved Issues 7

Defect SBC00004105 7

Defect SBC00004610 8

Defect SBC00004732 8

Known Issues 8

Defect SBC00005042 8

Revision History

Revision	Release date	Notes
1.0	July 2013	Release 3.1.0

Refer to www.dialogic.com for product updates and for information about support policies, warranty information, and service offerings.

Release 3.1.0

This document provides the following release information for the Dialogic® BorderNet™ 4000 Session Border Controller (SBC):

- Release Version Compatibility Table
- Maintenance Window Requirements
- New Functionality
- Resolved Issues
- Known Issues

Release Version Compatibility Table

Release	Supported Upgrade Path
1.0.x	1.0.5 > 2.2.9-004 or higher
2.0.x	2.0.x > 2.2.9-004 or higher
2.1.x	2.1.x > 2.2.9-004 or higher
2.2.x	2.2.9-004 or higher > 3.1.0
3.0.x	3.0.1-014 or higher > 3.1.0

Note:

- Release 2.2.9-004 is the minimum 2.2.x software version required to upgrade to Release 3.1.0. Systems with previous versions of the BorderNet 4000 SBC 2.2.x software must upgrade to Release 2.2.9-004 or higher in order to upgrade to 3.1.x.
- Release 3.0.1-014 is the minimum 3.0.x software version required to upgrade to Release 3.1.0. Systems with previous versions of the BorderNet 4000 SBC 3.0.x software must upgrade to Release 3.0.1-014 or higher in order to upgrade to 3.1.x.

Maintenance Window Requirements

Ongoing Calls will not be preserved upon failover during a Release 3.1 upgrade due to a mirroring version change in Release 3.1. Upgrades to Release 3.1 should be performed during a scheduled maintenance window.

New Functionality

The BorderNet 4000 SBC Release 3.1 contains the following new functionality:

- Overlapped IP Address
- IPPBX Registration Support
- IPsec Support
- External DNS Support
- Emergency Services
- Flexible Media Routing
- Enterprise Routing
- Filter Option for Reports
- User Security Enhancement
- List Users Currently Logged In With Ability to Close Sessions

Overlapped IP Address

The BorderNet 4000 SBC supports overlapping private networks with common IP addressing scheme. These topologies are frequently seen in managed service provider networks. Typically, VLAN tagging is used to clearly distinguish between different overlapping networks. The BorderNet 4000 SBC's interface definition and peer binding has been enhanced to include specifying the VLAN tag associated with each overlapped network. The BorderNet 4000 SBC uses this unique combination of SIP interfaces, peers, and the VLAN tags to route traffic between various overlapping networks.

IPPBX Registration Support

The BorderNet 4000 SBC can process SIP registration requests from both the consumer devices (e.g. IADs, soft phones, desk phones, mobile extensions, etc.) as well as from the IPBPBXs. IPPBX registration support is implemented as per the guidelines in the SIP Connect 1.1 recommendation and the RFC 6140—Registration for Multiple Phone Numbers in the Session Initiation Protocol (SIP) — standard. Specifically, the BorderNet 4000 SBC supports bulk registration of extensions from the IPPBXs.

IPsec Support

Internet Protocol Security (IPsec) is a suite of IETF-defined protocols for securing communications over the IP networks. IPsec protocols offer a range of security functions including data integrity, anti-replay protection, and confidentiality via authenticating and encrypting packets in each IP session. The BorderNet 4000 SBC supports IPsec Authentication Header (AH), which is used to authenticate and validate IP packets, as well as IPsec Encapsulating Security Payload (ESP). In the ESP mode, IP packets are encrypted. The BorderNet 4000 SBC supports manual keying and IKE v1. The BorderNet 4000 SBC IPsec implementation leverages built-in hardware encryption network processors included with the Network Interface Cards (NIC).

External DNS Support

In addition to local DNS capability, the BorderNet 4000 SBC supports the capability to query external DNS severs for URI resolution. The supported DNS queries include DNS SRV, DNS NAPTR, and DNS A

record lookups. The BorderNet 4000 SBC DNS implementation is IPv6-compatible and standards-based. The supported standards include RFC 3263, RFC 2782, RFC 2915 and RFC 3596. External DNS is useful for call routing, address resolution, and supporting remote peer redundancy.

Emergency Services

The BorderNet 4000 SBC has the ability to recognize emergency service calls based on Emergency Profiles configured on the system and can differentiate emergency calls from other calls.

The Call's Req-URI is checked for matching entries in the Emergency Profile configured for the Peer/Interface Service Profile. When a match is found, the call is marked as "Emergency" in the system and the resource priority header is added to the message. The Emergency flag is available for routing to provide custom behavior for such calls, and different Security Profiles can limit Emergency calls from the Peer/Interface.

Flexible Media Routing

The BorderNet 4000 SBC Release 3.1 introduces Flexible Media Routing, which enables the BorderNet 4000 SBC to intercept media on a per-call basis.

Enterprise Routing

The BorderNet 4000 SBC's Enterprise Routing achieves the maximum manipulation of digits, especially in the Called Party Identity (the user part of the Request-URI). This is accomplished via the BorderNet 4000 SBC SIP Profiler, which can be applied as part of the treatment parameter in the Advanced Policy.

Filter Option for Reports

The generic Report Filter in the WebUI has been enhanced to accept Time Range (Start and End) and Interface/Peer Name as user input (in addition to the Date filter) as search criteria.

User Security Enhancement

The Diagnostics menu required Administrative privileges in earlier releases. The user access enhancements now allow users to view Diagnostics information with read-only access.

List Users Currently Logged In With Ability to Close Sessions

The list of users currently logged into the BorderNet 4000 SBC can be viewed via the **Logged-In Users** screen in the WebUI. This feature provides Administrators with the ability to terminate currently active UI connections.

Resolved Issues

Defect SBC00004105

Issue

A 5-minute interval report could not be opened.

Root Cause

If the report was opened while the database was updating, the Report Controller generated an Error**: Unable to open report** exception.

Description of Fix

The code has been modified so that when the database is being updated, a more meaningful error message (**Error: Database is being updated. Please try the operation again later**) is generated.

Defect SBC00004610

Issue

An extension to the current session timer was requested.

Root Cause

The maximum session timer duration was limited to 7200 seconds (or 2 hours) in previous releases. Customers requested that this value be increased to 48 hours.

Description of Fix

The maximum session timer interval is now increased to 48 hours.

Defect SBC00004732

Issue

A software exception occurred after a provisioning change.

Root Cause

A race condition between call handling and provisioning triggered the software exception.

Description of Fix

The race condition is avoided by providing additional locking to ensure the exception does not re-occur.

Known Issues

Defect SBC00005042

Issue

GIT Remote was not setup on a HA system after rollback from 3.1.0 to 2.2.9.

Workaround

In a few instances during rollback operations, the Login Status updates ended with "Data merge conflicts" between the Active and Standby platforms. If sync errors occur during a failover after a rollback from 3.1 to 2.2.x/3.0, the Active platform can be "Reset" (if the other platform is in Standby state) from **System Information** screen. This will force the failover operation, and systems should automatically sync. An enhancement will be made in a future patch to automatically correct such merge conflicts.